

UNITED STATES OF AMERICA)
)
v.)
)
Manning, Bradley E.)
PFC, U.S. Army,)
HHC, U.S. Army Garrison,)
Joint Base Myer-Henderson Hall)
Fort Myer, Virginia 22211)

**STIPULATION OF
EXPECTED TESTIMONY**

SA John Wilbur

9 June 2013

It is hereby agreed by the Accused, Defense Counsel, and Trial Counsel, that if Special Agent John Wilbur were present to testify during the merits and pre-sentencing phases of this court-martial, he would testify substantially as follows:

1. I am currently the senior Special Agent (SA) at the computer forensic unit in the office of the Special Inspector General for the Troubled Asset Relief Program (TARP) at the Treasury Department. In this position, I collect and examine digital evidence to support criminal investigations. I have held this position since January of 2012. Previously, I was an SA for the Department of the Army's Criminal Investigation Command (CID), Computer Crimes and Investigative Unit (CCIU). I held that position from June of 2010 to January of 2012. As a CCIU SA, I investigated the unauthorized exfiltration of classified and sensitive data and the loss of personally identifiable information (PII) data worldwide. I also investigated intrusions into Army computer systems. I currently have over twenty years of law enforcement experience, fifteen of which have been primarily devoted to conducting complex criminal and administrative cyber-related investigations.

2. I have had substantial training to qualify me for my position. I received Department of State law enforcement training in 2005, CID law enforcement training in 2002, and Police Officer training in 1990. In addition to the evidence-handling training included in these courses, I also attended the "Advanced Crime Scene Investigations" course at the Federal Law Enforcement Training Center in Glynco, Georgia (May 2008). At the time of my involvement in this investigation, my cyber security and forensic evidence experience was extensive. Among other courses, I had attended multiple courses put on by Guidance Software, the makers of the EnCase forensic tool; I had attended the "Seized Computer Evidence Recovery Specialist Certification Course" (October 2001) at the Federal Law Enforcement Training Center; and I had attended "FT210, Windows Forensic Examinations" through the Defense Cyber Investigations Training Academy (DCITA). Further, I had obtained training in: "Law Enforcement Technology" (April 2002) through the University of Pittsburgh; "Advanced Data Recovery" (March 2001) and "Basic Data Recovery" (January 2000) at the National White Collar Crime Center; "Operational Information Security I and II" (July 2000) at the Defense Information Security Agency; and "Computer Search and Seizure" (June 2000) through the FBI Academy. I have continued to develop my skills and expertise. I have attended training in "Windows 7 Forensics" at Access Data (December 2010), the "Computer Incident Response Course" (April 2011) and a course on "Introduction to Networks and Computer Hardware" (December 2010) through DCITA.

3. My role in this case was to assist in witness interviewing and data collection. I collected evidence from the United States Central Command (USCENTCOM) server and from the

PROSECUTION EXHIBIT 72 for identification
PAGE OFFERED: PAGE ADMITTED:
PAGE 1 OF 5 PAGES

Department of State (DoS) server. In collecting the USCENCOM materials, I worked with Mr. Jacob Grant to collect both the server logs as well as information from a particular folder.

4. When collecting and handling evidence, I follow several general procedures. After collection, I review the evidence property custody document for the appropriate information. I fill out the date/time/place of collection and describe the evidence collected. I record, for example, serial numbers, markings for identification, and condition description matching the associated evidence. Further, I ensure that the necessary information, such as date and time, are properly and accurately recorded. Lastly, I maintain secure custody of the evidence prior to transferring it to another individual. In addition to following these procedures, when transferring to or receiving evidence from another person, I am also sure to properly sign, date, and note the reason for the transfer.

5. From the USCENCOM server, Mr. Grant and I collected information from the USCENCOM SharePoint site as well as the audit logs which track access to the site. I was interested in this information so that investigators could compare compromised information regarding the Farah investigation to information on the USCENCOM server, and so that investigators could identify computers which were used to retrieve potentially compromised material. Before Mr. Grant or I could accessed, imaged, searched for, or extracted any information, we needed special authorization from MG Jones, Chief of Staff, USCENCOM. CCIU forwarded a formal written request through the Office of the Staff Judge Advocate to the USCENCOM J-6 requesting release of this evidence on 9 August 2010. This request was approved on 19 August 2010. The same day, I worked with Mr. Grant to prepare for evidence collection by getting in order the equipment we would need for collection. Mr. Grant ensured that the laptop, hard drive, and cables we would need were clean of any data and ready for use.

6. The following day, Mr. Grant collected from the J-6 shop a DVD containing the audit logs for the USCENCOM SharePoint server. The logs show, among other things, the date/time USCENCOM documents were accessed on the SharePoint server, from December 2009 until August 2010. On 20 August 2010, he signed that evidence over to me. I took possession using the evidence handling procedures I describe herein including, but not limited to, documenting it on an Evidence Property Custody Document DA Form 4137 (labeled as document number (DN) 122-10 (BATES number: 00411111)). Later that same day, I properly signed that evidence over to the CCIU Evidence Custodian, Ms. Tamara Mairena. At no point did I alter the DVD or its contents. I have no reason to believe it suffered damage or contamination in any way.

7. In addition to collecting the logs, I worked further with Mr. Grant to access and collect information from the USCENCOM SharePoint collaboration space on the USCENCOM server. SharePoint is a tool produced by the Microsoft Corporation to create an internet interface which allows users with access to a SIPRNET website to collaborate, for example, by sharing files. The USCENCOM SharePoint itself is only accessible via SIPRNET, so a user must access it via secure systems and a proper security clearance. The server supporting it, from which Mr. Grant pulled the logs, is on virtual machines within a cluster, in a data center, on a storage area network (SAN). Only authorized USCENCOM Headquarters J-6 personnel are granted access to the facility. The data center is protected by badge access, cipher locks, video surveillance, and an access roster. This information was located on SIPRNET in the JAG folder

on the USCENTCOM SharePoint page. Mr. Grant assisted me in locating it on the system. We sat at his workstation to pull the folder contents. We knew where to focus our search based on Mr. Grant's SIPRNET webpage address identifications of the information at issue and because investigators in the case had cause to suspect the charged information was housed in the USCENTCOM JAG folder. In consultation with investigating forensic examiner SA Dave Shaver, we determined the most forensically sound way to collect the Farah information itself, as well as information about how it was accessible on SharePoint, was to navigate through the series of digital folders to download the Farah file itself. As we navigated through the folder structure on the SharePoint server, we took screenshots of the contents of each folder, before we entered the subsequent folder. A screenshot is the process of obtaining a digital copy of the computer screen, similar to a photograph.

8. During the morning of 20 August 2010, I connected, via a USB cable, a CCIU-issued Voyager drive dock to the laptop which accessed the SharePoint server via a USB cable. I connected a 400GB Seagate Barracuda, SATA hard drive (Serial Number: 3NFODYJ1) to the laptop using the drive dock and assigned that drive the letter "X". Using Microsoft's Internet Explorer, I navigated to the SIPRNET webpage "www.nonrel.cie.centcom.smil.mil". From this screen, I clicked on the "Organization" link. I created a screen capture of this page and saved it in a folder in the Desktop Directory called "screen shots". From this screen, I clicked on the "Special Staff" link. I created a screen capture of this page and saved it in the "screen shots" folder. From this screen, I clicked on the "Judge Advocate" link. I created a screen capture of this page and saved it in the "screen shots" folder. From this screen, I clicked on the "JA Document Page" link. I created a screen capture of this page and saved it in the "screen shots" folder. From this screen, I clicked on the folder icon "Investigations". I created a screen capture of this page and saved it in the "screen shots" folder. From this screen, I clicked on the folder icon "Farah". I created a screen capture of this page and saved it in the "screen shots" folder. The folder "Farah" contained the following sub-folders, "Admin Material", "Briefs", "Email", "Investigations Tabs", "Reports and EXSUMs", "Timelines", and "Videos". I navigated to each of the sub-folders and created a screen capture for each page then saved it in the "screen shots" folder. The screen shots showed how the SharePoint portal was arranged and the path to the "Farah" folder.

9. **Prosecution Exhibit (PE) 65 for Identification** is a computer printout that shows the file names and their associated paths that we navigated. It is a printout of a directory listing showing the filenames of each file and folder contained within the Farah folder on the USCENTCOM server with individual line numbers printed to the left of the listing. It lists the first level of subfolders within the Farah folder alphabetically, and then lists the filenames of the first subfolder. The document continues this process of listing subfolder names recursively, until all files and their filenames in all subfolders have been listed.

10. Later in the day on 20 August 2010, I recreated the folder "Farah" on the Desktop Directory of the laptop and included all of the subfolders that resided in the "Farah" folder. I then downloaded each individual file contained in the folder "Farah" into the same location inside the recreated "Farah" folder on the Desktop Directory of the laptop computer. After verifying that all of the files downloaded correctly, I installed EnCase version 6.14.3 on the laptop computer.

Using EnCase, I created a logical evidence file of the folder "Farah" and all of its sub-folders. The logical evidence file was named "JA-Investigations-Farah Folder.LO1". An MD5 hash of 46e11229a5d678cabf9c3fa6839f662c was obtained and recorded. The logical evidence file of the folder "Farah" was placed in a folder named "EnCase" on the root of the "X" drive connected to the laptop. I also copied the recreated "Farah" folder and all of the sub-folders and placed them onto the root of the "X" drive. Subsequently, the folder "Screen Shots" was then copied and placed on the root of the "X" drive as well.

11. When beginning the process of navigating through the JAG folder to obtain the Farah contents, I was not required to enter any login or password window on the main page. I was able to navigate to any page and access all folders and documents in the document library, including the SJA Investigations folder and the Farah folder without ever entering any authentication or credential information. In the Farah folder, all of the "video" files were password protected, including the a file named "BE22 PAX.zip" containing a video named "BE22 PAX.wmv". We therefore also requested and received the password to unlock the file named "BE22 PAX.zip" and the other videos from USCENTCOM. **PE 66 for Identification** is a CD containing the file named "BE22 PAX.zip" and the video file named "BE22 PAX.wmv". **PE 67 for Identification** contains the password for the file named "BE22 PAX.zip" which I received from USCENTCOM.

12. Later on 20 August 2010, I connected a second 400GB Seagate Barracuda, SATA hard drive (Serial Number: 3NFOHTG4) to the laptop using the drive dock and assigned that drive the letter "Y". I then recreated the process a second time placing the folder EnCase, containing the EnCase logical evidence file for the folder "Farah", the recreated folder "Farah", and the folder "Screen Shots" onto the root of the "Y" drive. The second evidence drive was created as a backup in case the first evidence drive suffered a failure.

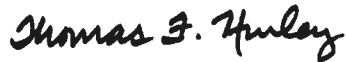
13. I later collected as evidence two SATA hard drives. These SATA hard drives each contained images of three folders (EnCase, Farah, and Screen Shots), copied from the USCENTCOM SharePoint server IP address 131.240.47.23, which was documented on Evidence/Property Custody Document (EPCD), Document Number (DN) 123-10 (identified at BATES number: 00411113). In processing this material, I handled and transferred the evidence as I have been trained. At no point did I alter any evidence I collected. I have no reason to believe this evidence was contaminated or damaged in any way. On 20 August 2010, I properly signed this evidence over to Ms. Tamara Mairena, the CCIU Evidence Custodian. I did not touch this evidence again.

14. Finally, I took possession of firewall logs from the Department of State from SA Ron Rock. I took possession of this evidence on 15 October 2010. He provided this information on a silver CD marked with the words "Wikileaks DoS Firewall Logs 13 October 2010". The CD had a red U.S. Government SECRET sticker on it. I recognize it as an official sticker because I have handled classified information before. I handled this evidence consistent with procedures as I have been trained and previously described. Upon taking custody, I checked to ensure the evidence I was receiving matched the description on the DA Form 4137, labeled as DN 151-10, Item 1 (identified at BATES number: 00411151). I checked the date, time, and other collection information. And finally, I signed in the "Received By" column. While in possession of this

evidence, I maintained positive control. I did not alter the information on the CD. I have no reason to believe this evidence was damaged or contaminated in any way. On 18 October 2010, I properly signed this evidence over to Ms. Mairena, the CCIU evidence custodian. I did not touch this evidence again. **PE 68 for Identification** is DN 151-10, Item 1.



ASHDEN FEIN
MAJ, JA
Trial Counsel



THOMAS F. HURLEY
MAJ, JA
Military Defense Counsel



BRADLEY E. MANNING
PFC, USA
Accused